AU/ACSC/BAKER/AY15

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

CYBERSECURITY FOR CRITICAL INFRASTRUCTURE

by

Christopher J. Baker, Major, USAF

A Research Report Submitted to the Faculty

In

Partial Fulfillment of the Graduation Requirements for the Degree of

MASTER OF OPERATIONAL ARTS AND SCIENCES

Advisor: Wing Commander Graem M. Corfield

Maxwell Air Force Base, Alabama

April, 2015

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the United States government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

TABLE OF CONTENTS

Page

Abstract

The Sony cyber incident in November 2014 has inspired questions as to the best method of providing cybersecurity in the United States. Specifically, who is best postured to provide cybersecurity and on what parts of the cyber domain should this security be focused? The United States government takes seriously the threat of cyberspace attacks; however, not all cyberspace incidents should result in the initiation of armed conflict. This paper argues the Sony cyber incident should not be considered a cyberspace attack as it relates to the law of war. It then reviews the current role of the Department of Homeland Security with respect to cybersecurity for critical infrastructure and key resources. Next, it will review the authorities for states' National Guard units to provide cybersecurity for critical infrastructure and key resources. Finally, this paper discusses how the National Guard is best postured to safeguard the critical infrastructure and key resources within their borders.

Introduction

On 24 November 2014, Sony Pictures Entertainment (Sony) experienced what it referred to as a "brazen cyber attack."[1] Sony informed its employees the perpetrators may have obtained their personally identifiable information, such as social security numbers; bank account information; credit card information for corporate travel and expense; usernames and passwords; health and medical information; and other employment-related information.[2] The cyber infiltration also attained embarrassing emails among Sony executives.[3] The incident highlighted several issues relating to the cyber domain, including what constitutes a cyberspace attack and what role the government, in particular the military, should play in protecting private individuals and corporations from outside threats.

There are relatively few laws relating to the internet and cyberspace. Current federal law includes the CAN-SPAM Act,[4] the Computer Security Act of 1987,[5] the Children's Online Privacy Protection Act of 1998,[6] the USA PATRIOT Act, the Fair Credit Reporting Act, the Freedom of Information Act, and the Gram-Leach-Billy Act.[7] Many states have passed laws relating to disclosure of personal information to consumers and identity theft, and every state has enacted laws to address cyber stalking or cyberbullying.[8] Although there are more than 50 federal statutes addressing various aspects of cybersecurity either directly or indirectly, there is still no predominant cybersecurity legislation in place.[9]

In the event of a true cyberspace attack against civilians, corporations, or critical infrastructure, the United States military is limited in what it can defend.[10] In the same vein, the role of the National Guard in Title 10 status would be similarly limited in defending purely non-Department of Defense (DOD) cyber networks.[11] Whereas in their respective states and in their status under Title 32 Guardsmen have different legal authority, particularly with respect to

homeland defense activities in general and cyber operations specifically.[12] It is important to remember that according to statute as well as joint doctrine, the Department of Homeland Security (DHS) has the responsibility to secure United States (US) cyberspace by "protecting non-DOD [United States Government] (USG) networks against cyberspace intrusions and attacks," while the responsibility to protect other non-USG networks lies with those who own the networks.[13] However, the Under Secretary of the DHS is also required to work with *state and local governments* to develop, update, maintain, and exercise "adaptable cyber incident response plans to address cybersecurity risks to critical infrastructure."[14] Most of DHS's statutory responsibilities involve planning, consulting, coordination with other Federal entities and state and local governments, as opposed to providing cybersecurity to critical infrastructure assets and key resources (CI/KR).[15] This leaves a void in responsibility for actually protecting non-DOD and non-USG CI/KR. The National Guard should be utilized in their State Active Duty status to protect non-DOD CI/KR in cyberspace.

This paper will briefly address why the Sony incident was not a cyberspace attack as it relates to the law of war. It will next examine the role of DHS vis-à-vis cybersecurity of CI/KR. Additionally, it will examine and compare the authorities of states' National Guard units to engage in cybersecurity of CI/KR. Finally, it will discuss why the National Guard is best positioned to safeguard CI/KR located within their borders.

Was the Sony Incident a Cyber Attack?

Defining Cyber Attacks

There is a tendency among the media and the public to label all cyber incidents as "cyber attacks." This mislabeling may be a result of ignorance of proper definitions, convenient stereotyping of network incidents into a common term, or perhaps a visceral reaction to the

feeling of vulnerability experienced by victims of such incidents. Since words have meanings, it is important to use the proper vernacular when describing such events. According to Joint Doctrine, cyberspace attacks include actions designed to create denial effects (i.e., degrade, disrupt, destroy) or manipulation of control or change information, information systems, or networks.[16]

The Tallinn Manual on the International Law Applicable to Cyber Warfare narrows the definition of a cyberspace attack to a "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[17] Although the Tallinn Manual is not binding on the U.S. military, it is a more useful definition when considering what, if any, actions to take in response to such an incident. Both definitions fail make any distinction as to the object or target of the attack. As such, the Sony incident could be considered a cyberspace attack because one of the effects of the incident was the destruction of some of Sony's computers. One can see how the definition of a cyberspace attack should consider the victim, as a state should not consider itself "attacked" if some computers of an international corporation with offices within that state should incur a destructive effect as a result of a cyberspace attack. Conversely, if a foreign state were to create destructive effects of a nuclear power plant which results in the loss of tens of thousands of lives, a state would be justifyied in considering such a situation an attack.

The Sony incident involved a network intrusion and the theft of data. Although JP 3-12(R) has several references to "intrusions", there is no doctrinal definition of a "computer intrusion."[18] While the Tallinn Manual also does not define an "intrusion," it does opine that "network intrusions, the deletion or destruction of data (even on a large scale), computer network exploitation, and data theft" do not rise to the level of an attack. The definition of an attack in

general warrants further explanation, as it brings into play principles of the law of armed conflict (LOAC).

Cyberspace Attacks and the Law of War

There are two areas of international law which pertain to conflicts: *jus ad bellum* and *jus in bello*. Although customary international law was developed long before the advent of cyberspace operations, cyberspace operations are subject to both areas of the LOAC.

Article 2(4) of the United Nations Charter provides: "All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any manner inconsistent with the Purposes of the United Nations."[19] Additionally, Article 51 states: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."[20] Moreover, Article 41 provides: "The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."[21]

The importance of whether an action in cyberspace is an attack lies with the permissible responses a state may take after falling victim to such an incident, for LOAC could provide states with the right to respond with armed force to a cyberspace attack. Although the United Nations Charter admonishes states generally from the "use of force" against other states, exceptions to the general rule are the use of force as authorized by the Security Council and Article 51's self-

defense clause. Unfortunately, the Charter does not define "use of force" or the use of "armed force." One would not want to use a definition of "use of force" that is defined too broadly. According to General Keith Alexander, DOD systems alone are probed more than 6 million times each day.[22] This number does not include probes of other USG networks, nor does it include probes of CI/KR systems. Moreover, one can assume as technology has improved over the last five years the number of probes has also likely increased with time. Accordingly, one must be judicious in what he or she considers an attack, a use of force, or a use of armed force.

If one were to define any probe as a "use of force," the definition would be untenably worthless. Even the DOD definition of a cyberspace attack (i.e., deny, degrade, disrupt, destroy, or manipulate) is quite broad. The Sony incident provides an example of what not should be considered a "use of force." First, it does not appear the intent of the intrusion was one of war. When assessing a proper response it is crucial to determine whether the incident was one with criminal intentions or war intentions. Intrusions such as those involving the theft of information, "intelligence gathering, espionage, or periodic disruptions or denials of nonessential cyber services" may be extremely vexing for the victims of the incident.[23] A temporary denial of access to a news network's website can be frustrating for those wanting to read the news, but it should not be considered a use of force. One could argue stealing data or manipulating information could demonstrate intent for war if the data stolen pertained to strategic plans or weapon systems designs from the defense industrial base. However, this is more akin to espionage, which does not evince intent for war.

The second reason why the Sony incident should not be considered a use of force for LOAC purposes is because Sony is not part of the CI/KR system. It does not provide any cyber services essential to the U.S. In 1996, President Clinton issued Executive Order 13010, in which

he explained his definition of critical infrastructure as infrastructure "so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[24] Examples of this infrastructure include "telecommunications, electric power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency systems (including medical, police, fire, and rescue), and continuity of government."[25] In 2013, President Obama issued Executive Order 13636 in which he defined critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[26]

If the Sony incident and those similar to it should not be considered a use of force for LOAC purposes, one must understand what should be considered a use of force for such purpose. The United Nations Charter and customary international law have not provided a definition, but many legal scholars have debated the issue at length. Gary Solis provides a useful definition: "[a] cyber[space] attack constitutes a "use of force" if undertaken by a state's armed forces, intelligence services, or a private contractor whose conduct is attributable to the state, and its scale and effects are comparable to non-cyber operations that rise to a level of a use of force."[27] The latter clause of this definition echoes the definition espoused in the Tallinn Manual.[28] Solis further argues cyberspace attacks should be considered the use of armed force if the attack is one "that kills, wounds, or destroys …, just as kinetic weapons causing the same results, would be considered an armed attack."[29] Although not globally accepted, these definitions will be adopted for purposes of the paper. These definitions serve well to eliminate many cyber intrusions from the realm of cyberspace attacks.

The U.S. takes seriously the threat of cyberspace attacks to its CI/KR, and it is U.S. policy to keep its options open to protect CI/KR.[30] Executive Order 13231, issued in the wake of the terror attacks of September 11, 2001, provides it is U.S. policy to protect against "disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the [U.S.]."[31] Moreover, DOD policy warns the DOD will "work with interagency and international partners to … oppose those who would seek to disrupt networks and systems, dissuade and deter malicious actors, and reserve the right to defend these vital national assets as necessary and appropriate."[32]

The Department of Homeland Security's Role

As stated, DHS is currently the executive agency assigned the responsibility to oversee critical infrastructure protection and cybersecurity.[33] Title 6 of the United States Code enumerates DHS's responsibilities relating to intelligence and analysis and infrastructure protection. DHS is charged with accessing, receiving, and reviewing law enforcement, intelligence, and other information to detect and understand terrorist threats.[34]

Additionally, DHS is responsible for conducting comprehensive assessments of CI/KR vulnerabilities and to develop a comprehensive plan to protect said resources.[35] It is further charged with the responsibility of recommending measures necessary to protect CI/KR.[36] However, DHS is not charged directly with providing cybersecurity to the CI/KR. In coordination with other Federal departments and designated Sector-Specific Agencies (SSAs), DHS provides analysis, expertise, and other technical assistance to CI/KR owners.[37] It also coordinates Federal Government responses to significant cyber or physical incidents affecting

CI/KR consistent with statutory authorities and provides annual reports on the status of CI/KR efforts as required by statute.[38]

In Presidential Policy Directive (PPD) 21, President Obama identified 16 critical infrastructure sectors and designated Federal SSAs for each sector. Each SSA is responsible for providing "institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector."[39] Both PPD-21 and the National Infrastructure Protection Plan (NIPP) explain the agencies responsible for each critical infrastructure sector: DHS is the SSA for chemical, commercial facilities, communications, critical manufacturing, dams, emergency services, information technologies, and nuclear reactors, materials, and waste; Department of Agriculture and Department of Health and Human Services are the SSAs for food and agriculture; DOD is the SSA for the defense industrial base; Department of Energy is the SSA for energy; Department of Health and Human Services is the SSA for healthcare and public health; Department of Treasury for financial services; Environmental Protection Agency for water and wastewater systems; DHS and General Services Administration for government facilities; and DHS and Department of Transportation for transportation systems.[40]

Many aspects of the CI/KR are privately owned. Accordingly, most of the plans and efforts for critical infrastructure security and resilience established by the NIPP are voluntary. The NIPP recognizes that when private sector owners collaborate voluntarily with the government, the national goal of security and resilience of CI/KR is more effectively recognized.[41] It also establishes seven core tenets the CI/KR community should consider when developing plans for CI/KR security and resilience.[42] The fourth tenet states: "The partnership approach to critical infrastructure security and resilience recognizes the unique perspectives and

comparative advantages of the diverse critical infrastructure community."[43] It acknowledges the abilities and capabilities the private sector, nonprofit sector, and all levels of government offer this effort.[44] Similarly, tenet five discusses the importance of partnerships at the local level throughout the country to strengthening security and resilience.[45]

The ability for public and private sector CI/KR owners and operators to cooperate and make risk-informed decisions is essential for the effort to strengthen CI/KR security and resilience.[46] Ultimately, individual entities, especially private sector entities, are responsible for managing risks to their organizations.[47] Private entities generally will measure and manage risks based on a variety of factors (including profit), and different entities will have different tolerance for risk. The NIPP proposes a tailorable risk management framework to provide flexibility for use in all sectors; however, use of the framework is not binding.[48] Effective partnerships coupled with responsible policies and timely information sharing can improve these entities' abilities to understand threats, vulnerabilities, and consequences.[49]

The NIPP also directs efforts to realize national goals of improving CI/KR security and resilience. It addresses the importance of Federal departments and agencies engaging with state, local, tribal, territorial, (SLTT) and regional governments and private sector partners to work together in several lines of effort. One of the NIPP's proposed actions involves building upon partnership efforts.[50] One particular call to action relates to empowering local and regional partnerships to build capacity nationally.[51] It recognizes most cyber incidents (and attacks) are local in nature; that is, the effects felt are generally limited to a network in one area as opposed to affecting, for example, all servers across the country. Accordingly, local and regional partnerships are crucial to integrating CI/KR security and resilience.[52] The local government partners advance national aims by working with and helping private entities secure CI/KR.

Moreover, this call to action is designed to advance regional CI/KR preparedness and will involve SSAs working with states toward this end.[53]

The current administration appears committed to facilitate local-level partnerships to improve CI/KR security and resilience through cybersecurity. On 13 February 2015, President Obama issued *Executive Order: Promoting Private Sector Cybersecurity Information Sharing*, in which he recognized the need to address cyber threats through continued cooperation between the government and private companies. The Order, which builds upon Executive Order 13636 and PPD-21, is designed to encourage near real-time collaboration and information sharing of cybersecurity risks among private companies, nonprofit organizations, and the government.[54] Additionally, the Order is designed to "encourage the voluntary formation of such organizations, to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis."[55] The DHS is tasked to "strongly encourage" the creation of "Information Sharing and Analysis Organizations (ISAOs)".[56] The ISAOs may be organized based on sector, vulnerability to threats, geography, or any other basis; and membership can consist of entities from the public, private, and nonprofit sectors.[57]

Many of the SSA-specific plans also envision coordination with SLTT governments. For instance, the IT Sector Specific Plan recognizes state and local governments provide a variety of services, including IT services, designed to meet the needs of their citizens, businesses, and employees.[58] The goals and objectives of the IT Sector plan include collaboration between public and private sector partners to "prevent, prepare for, protect against… nationally significant events, technological emergencies, or presidentially declared disasters that threaten, disrupt, or cripple IT Sector functions."[59] Similarly, the Chemical Sector Plan identifies SLTT

as the "front line of defense" in preventing harm in the Chemical Sector and responding to secure this piece of critical infrastructure.[60]

The Role of the National Guard

Additionally, some Sector-Specific Plans, such as the Nuclear Reactors, Materials, and Waste Sector; the Transportation Systems; the Commercial Facilities; and the Energy annexes, currently identify the National Guard's role in providing for physical security for CI/KR facilities as well as responding to incidents involving CI/KR. Although these roles do not currently include providing cybersecurity, the plans acknowledge the National Guard's value with regard to securing CI/KR. They also do not specifically preclude the National Guard from participating in cybersecurity. It is not a stretch to argue the additional value the National Guard could play with regard to cybersecurity when they already provide for the physical security of the exact same infrastructure. The National Guard is uniquely positioned to be a force multiplier in the area of cybersecurity. One obvious reason is its composition. The National Guard fills its ranks primarily from citizens who work principally in the private sector.

The former commander of USCYBERCOM envisioned leveraging Guardsmen into the sub-unified command, stating that "it is our intent to have Guard forces align regionally to help in prevention, protection and recovery operations. This will be a key inter-government partnership."[61] In the same vein, the 2014 National Defense Authorization Act (NDAA) required the DOD to develop a concept of operations and a concept of employment for cyber forces, to include an analysis on the reserve components' role.[62] The NDAA also required states, through the Council of Governors, to provide an assessment of state cybersecurity capabilities, as well as an evaluation of state cyber needs the private sector cannot fulfill.[63] Furthermore, the NDAA requested an assessment "whether the National Guard, when activated in a state status

(either State Active Duty or in a duty status under Title 32…) can operate under unique and useful authorities to support domestic cyber missions and requirements of [USCYBERCOM]."[64]

The DOD has begun integrating the reserve component under the cyber umbrella. Part of the Army's plan includes standing up one full-time and as many as 10 part-time Army National Guard cyber protection teams (CPTs), which could support homeland defense, civil support, or other missions in Title 10 or Title 32 status.[65] The Air Force similarly plans to use National Guard CPTs as part of their main cyber force.[66]

National Guard Authority

The National Guard derives its authority from Title 32 and from each respective state's laws. While Title 32 recognizes the important role the National Guard plays as the first line of defense of the United States, the state codes provide more detail as to under what circumstances they will be activated.[67] Although states differ in their specific verbiage, most states authorize the governor of that state to call out forces when certain criteria are met. Alabama permits the governor to call out forces whenever there is an "insurrection or outbreak of a formidable character which has overawed, or threatens to overawe, the ordinary civil authorities;" in cases of disaster in which local authorities have attempted and failed to quell; to enforce the law; and preserve the peace; when the urgency is great.[68] Alaska allows the governor to call out forces in cases of "war, disaster, insurrection, rebellion, tumult, catastrophe, wildland fire, invasion, or riot;" when the governor believes civil authorities will imminently fail to preserve law and order or protect life and property.[69] States such as Arkansas, California, Connecticut, Delaware, Missouri, Rhode Island, and Washington permit the governor to call out forces under similar circumstances.[70]

One of the states providing more breadth of opportunity for the governor to call out forces is Arizona. Arizona allows the governor to call out forces during a state of war or a state of emergency, the latter of which includes "conditions of disaster or of extreme period to the safety of persons or property within the state caused by air pollution, fire, flood or floodwater, storm, epidemic, riot, earthquake or other causes … which are or are likely to be beyond the control of the services, personnel, equipment and facilities of any single county, city or town, and which require the combined efforts of the state and the political subdivision."[71] While this definition is more broad that other states, it omits any reference to utilizing Guard forces to protect CI/KR.

Michigan is a state that appears to be on the cutting edge when it comes to cybersecurity of CI/KR. Although its statute permitting the governor to call out forces includes language similar to many other states (e.g., cases of "riot, tumult, breach of peace, resistance or process"), it also permits calling out forces in "time of actual or imminent public danger, disaster, crisis, catastrophe or other public emergency within this state or to respond to acts or threats of terrorism or to safeguard military or other vital resources of this state or of the United States."[72] Vital resources are defined as "public or private building[s], facilit[ies], property, or location[s] that the governor considers necessary to protect the public health, safety, and welfare of the citizens of this state."[73] Currently, Virginia is the only other state to include defense of vital resources in its list of circumstances permitting the governor to call out forces.[74]

Current National Guard Cybersecurity Utilization

The various governors are working to address cybersecurity within their states, several of whom are integrating the National Guard. In Missouri, the National Guard has established a cyber-threat response team designed to respond to cyber threats or attacks at both the state and

national level.[75] The Delaware Air National Guard has the 166th Network Warfare Squadron, a squadron that performs offensive and defensive cyberspace operations.[76] Additionally, Maryland utilizes its Air National Guard's 175th Network Warfare Squadron to support its cybersecurity assessments.[77] The 175th engages in training exercises with state agencies, simulating attacks on their networks.[78] The state agencies use the lessons learned in the exercise to reduce risk through technical and procedural countermeasures.[79] Moreover, the 262d Network Warfare Squadron, a Washington Air National Guard unit that draws upon the rich computer-based talent pool of the Seattle area, detects, monitors, and defends against cyber threats.[80] In February 2015, the Army National Guard announced Michigan would host one of its first three CPTs.[81] Once the CPT is fully trained, it will conduct defensive cyberspace operations, perform readiness inspections and vulnerability assessments, and perform other cyber roles and missions.[82]

In addition to leading the way in Michigan's enumerated authority to call out forces to protect CI/KR, Michigan also is also at the forefront of building public-private collaboration for cybersecurity. In early 2015, Michigan Governor Rick Snyder released *Michigan Cyber Initiative 2015 – Leading the Nation: An Interagency, Public-Private Collaboration*, which builds upon a 2011 state initiative. While the initiative recognizes the private sector is responsible to ensure their information technology systems are protected, it recognizes the nexus between the corporate community and the public sector when it comes to a private company's ability to maintain secure systems.[83] In addition to creating an award-winning website to inform people about cyber protection, Governor Snyder established the Michigan Cyber Command Center to address cybersecurity threats to both the government and citizens in Michigan.[84] Michigan also developed the Michigan Cyber Civilian Corps to work with government, private

entities, and educational institutions to develop and cultivate "rapid response teams" to respond to major cyber incidents.[85]

Michigan does not just focus on reaction to cyberspace attacks. It also built a cybersecurity range to meet the needs of CI/KR defense, homeland security, criminal justice, and education.[86] The Cyber Range project is an all-inclusive undertaking with input from and cooperation with government, the National Guard, universities, community colleges, K-12 schools, and the private industry.[87] Michigan has established cyber range extension sites at nearly all National Guard bases in the state to train guardsmen in cybersecurity disciplines and to host cyber exercises with partners within the state and private businesses.[88] Michigan intends to equip all National Guard bases in the state with extension sites.[89] In this vein, Governor Snyder has assigned the Michigan National Guard the task of "support[ing] the prevention, protection, mitigation, and response to cyber incidents."[90]

Additionally, Michigan hosts a variety of public-private collaborations designed to create a "cyber-resilient ecosystem."[91] The Michigan Public Service Commission collaborates with utility and other CI/KR providers to protect energy control systems from cyberspace attacks and accidents that could have large impacts on public health and safety.[92]

The Michigan National Guard has gained considerable valuable cyberspace defense experience in the past three years. In June 2012, the Michigan National Guard contributed to USEUCOM Cyber Endeavour 2012, strengthening the cyber defense capacity of 40 NATO and partner nations.[93] In September, the Guard provided mission assurance and intrusion detection support at the Democratic National Convention in Charlotte, North Carolina.[94] Additionally, it participated in Cyber Flag 2013, leveraging various capabilities to ascertain presence rapidly,

prevent lateral movement, and remediate malicious logic in the Cyber Network Operations and Defense competencies.[95]

In 2013, the Michigan National Guard provided intrusion detection capabilities and skillsets to four Joint Incident Communications Capabilities deployed throughout the National Capital Region in support of the Presidential Inauguration.[96] In September of that year, the Guard participated in Cyber Shield 2013 in Fairfax, Virginia. Participants joined a mission assurance team that provided computer emergency response team and computer network defense service provider support.[97] In April 2014, Michigan's Joint Cyber Operations Team joined more than 300 Air and Army National Guard cyber warriors from 35 states for Cyber Shield 2014, implementing cyber defense tactics, techniques, and procedures and reporting requirements against simulated attacks on the DOD Cyber Security Range.[98] It also participated in Cyber Endeavour 2014.

Leveraging the Guard

Despite Michigan's extensive utilization of its National Guard, the state has not gone as far as to specifically designate the Guard as *the* entity to defend its state CI/KR. Michigan and other states should leverage the National Guard in this role. Michigan and Virginia currently have authority in place for the governors to call out guardsmen to defend CI/KR. Admittedly, the other states would have to change their state codes or loosely interpret other provisions that provide the authority to call out forces, which could be possible especially considering most state laws also consider the governor's decision that an emergency exists as final.

Once the states have the authority to call out forces to active service to defend CI/KR, each state should strive to enhance its National Guard cyberspace capabilities. Vanguard states such as Michigan or Virginia can serve as a model for training and utilization for other states.

Governments at all levels recognize the need for partnerships at the local level to address their specific risks, but they also recognize the internet is connected and these partnerships must utilize information from outside the local area and the state to provide optimal defense to the systems connecting their CI/KR.

Additionally, since Guard members are citizens working in the local community in their civilian capacity, they would be able to develop more effective relationships with local private CI/KR industry leaders. These relationships would in turn help explain the importance of cooperation and information sharing between those industries and the local, state, and federal governments. Moreover, some Guardsmen might already be employed as information technology specialists in those industries, and that nexus would further serve the effort to encourage both information sharing and acceptance of defense from National Guard units.

The National Guard differs from the Title 10 active duty military in a very important way: the *Posse Comitatus Act* does not apply to them.[99] Accordingly, the National Guard in its State Active Duty status can perform both defense and police functions. Just as a Guard unit activated to respond to a physical disaster or riot can serve to defend people and prevent destruction of physical property and enforce the state's laws, a cyber-unit could serve to defend people and prevent destruction of physical and intellectual property by defending CI/KR networks. It is also not prohibited from enforcing state laws. This means the units could not only defend networks but they could also be involved in search for or apprehension of offenders who infiltrate CI/KR networks.

Detractors may argue the responsibility to protect CI/KR networks rests and stops with those particular private entities. States do not post National Guard units outside shopping malls to prevent burglary, nor do not deploy tanks at restaurants to defend against vandals. The

responsibility to provide security for those events and industries rests primarily with the businesses providing those services. Accordingly, taxpayer money should not be spent providing cybersecurity to CI/KR industries.

There are two problems with this argument. The first problem is economic reality. The role of government is to protect the civilians of which it is composed. The role of businesses is to provide a service in order to maximize profit. Since the goal of a private business is to maximize profit, it will make decisions with the bottom line in mind. Cybersecurity costs money. If a chief executive officer (CEO) or chief financial officer (CFO) of a business is weighing the option of whether to provide cybersecurity and, if so, to what extent should that cybersecurity be provided, he or she will look at how much money that decision will cost. He or she will also probably look at the risk to the bottom line by not taking action. If the amount of investment in cybersecurity is high and risk of loss is low, the CEO or CFO may decide against acquiring and providing robust cybersecurity.

Private companies that run CI/KR industries are no different from other commercial entities. The CEO's and CFO's goal is to maximize profit for the company. If they make a business decision that will cause them to lose money, they risk losing their jobs. Moreover, there have not been any major cyberspace attacks on CI/KR industries. Accordingly, the risk of business loss of not improving cybersecurity is low. When CEOs and CFOs compare the cost of providing security with the concomitant reduction in profits due to the expenses incurred from providing the security, they may be disinclined to provide additional cybersecurity.

The second problem with the complaint that states should not use the National Guard to protect CI/KR networks is with the price of failure. If a corporation such as Burger King fails to provide adequate cybersecurity to its networks, its risks include some potential loss in business.

But past examples show corporations can recover from such incidents. Generally, however, no one will die if Burger King's networks are subject to a cyberspace attack. Conversely, if a CI/KR entity is subject to a cyberspace attack, public safety is at risk. A cyberspace attack on the SCADA network of a water refinery could affect clean drinking water. A cyberspace attack on power companies during the winter could lead to many deaths due to exposure, not to mention the potential loss of life at hospitals due to lack of life support. The potential destruction resulting from an attack on a nuclear power plant or dam would be devastating. The potential risk justifies use of National Guard forces to protect these systems.

Another argument against using the National Guard is similar to the first: government should not be involved in providing cybersecurity to private companies. Allowing the government to provide cybersecurity would mean providing the government access to those networks. Those networks contain private information. This information could provide the government with evidence of personal behavior, not to mention personal information about customers. The government should not be able to access this information without a warrant. Moreover, the government will abuse this information and use it to infringe upon people's liberty.

This argument also fails to pass muster. First, this paper assumes the CI/KR industry consents to the National Guard providing cybersecurity. Additionally, only a few CI/KR industries store personally identifiable information, and there is no information on private customers within these networks that would infringe upon someone's liberty or privacy. Moreover, there is no information contained within these networks that the government could not get already without a warrant. Personal information such as phone numbers and addresses are available in phone books or on the internet, all of which is accessible without a warrant.

Information such as dates of birth or social security numbers is contained in public records which the government could access without a warrant. Other information these companies possess is information on the amount of water or energy a customer is using. The government could get this information simply by walking up to a house each day, week, or month and reading the meters outside a house. A warrant is not required to do such a check. Finally, SCADA networks control machines. If cybersecurity was confined to defense of SCADA networks, there should be no private information to be accessed or discovered.

Additionally, simply knowing how much power or water someone is using does not reflect what someone is doing privately inside their house. Certainly, an extremely high amount of energy or water use could result from a nefarious activity, but that information alone does not tell the government the exact nature of the activity and it would not be grounds to get a warrant to search the premises.

This argument is strongest with regard to the financial sector. The inflow and outflow of money and the people or entities with which that money is exchanged does have more meaning than the information contained in other sectors. However, this does not mean the state would have to employ the Guard in the same way for every sector. With regard to the financial sector, the Guard could focus primarily on barriers to entry as opposed to detecting a threat in the system. Additionally, banks and other financial institutions have more incentive to spend money on cybersecurity than other industries. These institutions rely on loans from their customers to make money. If customers do not believe their money is secure with that financial institution, they will take their money elsewhere. Each institution will still likely have differing levels of risk they are willing to accept, but their cost-benefit analysis is much more amenable to providing cybersecurity than other CI/KR sectors.

One could also argue allowing the National Guard to provide cybersecurity would be tantamount to nationalizing the resource. Further still, one could argue this practice would establish the beginning of a police state. As to the first concern, if an armed policeman or (in case of riot, insurrection, etc.) an armed National Guard member were posted at a bank to keep openly armed robbers from entering while allowing legitimate patrons to enter, no one would consider the presence of the guard to be a nationalization or taking of the bank. The principle is the same with cybersecurity. Cybersecurity would be aimed at precluding people who are not entering the network to perform legitimate business relations with the CI/KR entity. The argument that these actions would result in a police state equally fall flat as merely fear mongering. The goal of this entire course of action is to protect CI/KR and, by extension, the public. Utilizing guardsmen to provide this security effort does nothing to limit people's rights or to infringe upon the due process of law.

A question remains of how to incentivize civilian IT experts to join the National Guard. Although some may be motivated by patriotism to serve, many would not be. Moreover, these civilians likely are compensated very well in their civilian capacity and would not likely be motivated to give up their personal time for whatever military pay they would receive. One potential way to attract this talent would be to authorize a tax incentive similar to the tax benefits received when service members are deployed. Another potential incentive would take the form of tax breaks and credits to help reduce the amount of taxes they pay on their civilian salaries. Specifically, the incentive could be designed as such: for each day worked in Guard status, a commensurate number of days for their civilian job would be tax-free. Accordingly, in addition to the military salary, they would receive a tax break. These efforts could provide the stimulus to draw in this talent base without costing the government additional money for bonuses.

Finally, one could argue the effort would fail because if the Guardsmen are playing this role in State Active Duty status, there is no national command and control directing the effort. This would make integration and unity of effort much more difficult, if not impossible. However, there is nothing to stop the Council of Governors from adopting consistent practices and integrating the guidance the DHS has established on information sharing and coordination. Many states already coordinate and exercise together. It is in each state's interest to employ best practices to secure these resources. Similarly, many states have agreements in place to assist each other in the event of a natural disaster. These agreements could be amended to provide for coordination in the event of a cyberspace attack. Still, even assuming coordination fails; one could still argue a lack of coordination provides variety. This variety could make it more difficult for a cyberspace attack to affect each state's CI/KR networks. If each state used slightly different cybersecurity methods, attackers would have to use different methods to take down a dam in Alabama from the methods to take down the Hoover Dam.

Ultimately, the goal among the states should still be unified action, and states would likely be motivated to share information and coordinate to ensure a problem in one state does not spill over into other states. The Council of Governors could develop a coordination plan to address actions to be taken in the event of an attack. Moreover, the National Guard Bureau could develop a plan to ensure unity of effort among the states in this critically important area. Although both the Council and the National Guard Bureau are capable of coordinating efforts, the latter would be more effective at publishing a coherent an inclusive plan to orchestrate the efforts of the states toward the end of unified action.

Conclusion

Conclusions

The cyber incident against Sony should not be considered a cyberspace attack for law of war purposes. Although it amounted to more than a mere intrusion and resulted in physical damage to some computers, an incident of this nature on a private company such as Sony should not be considered a use of force or armed attack. However, even though the Sony incident should not be considered an armed attack there may be cyber incidents in the future that will be attacks with respect to the laws of war. The Department of Homeland Security is the executive agency charged with coordinating cybersecurity for the country's critical infrastructure and key resources, but its role is largely one of coordination and information gather and sharing. Moreover, it does not have the budget or manpower to provide cybersecurity for every part of the nation's critical infrastructure. The National Guard is the logical choice to provide cybersecurity for these entities.

Recommendations

State governors should develop cybersecurity units in their National Guard forces, and they should utilize their authority to employ their respective forces to provide cybersecurity for CI/KR within their states. Vanguard states such as Michigan and Virginia should leverage authorities already in place to provide cybersecurity to these industries. The other states should follow their lead, develop the authorities, train their units, and continue to coordinate and collaborate with CI/KR industries in their states. They will then be positioned to take the next step and provide cybersecurity to those entities. The states could develop a phased approach based on the amount of resources it can bring to the fight, focusing first on finances, water, and entities providing power. Additionally, the Council of Governors and the National Guard

Bureau should develop guidance for the states to ensure unity of effort in the event of a large-scale disaster or attack.

Summary

The National Guard is unique in that it can serve both its state governor and the President of the United States. When this role is combined with its ability to recruit and retain specialists from IT and related fields, the National Guard provides an ideal opportunity to become a force multiplier in the realm of protecting states' CI/KR. Many states have authorities in place and have begun to establish units designed to serve this purpose, but more states must join the cause. In their State Active Duty status, the National Guard is the government entity in the best position to provide cybersecurity for CI/KR networks. No other government entity is designed or organized in such a way that its personnel live near and interact with the entities the organization is tasked to defend. The National Guard is known for its ability to protect the communities in which they live. Providing cybersecurity for CI/KR networks in their states is the next logical step in the Guard's role of protector.

Notes

1. "Sony Pictures Entertainment Notice Letter," 8 December 2014.
2. Ibid.
3. Michael Cieply and Brooks Barnes, "Sony Pictures Demands That News Agencies Delete 'Stolen' Data." *New York Times*, 14 December 2014.
4. Title 15, United States Code (U.S.C.), sec. 7704, a law that sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations.
5. Title 15, U.S.C., sec 272. This act gave the National Institute of Standards and Technology responsibility for developing security standards for federal computer systems, except the national security systems that are used for defense and intelligence missions, and gave responsibility to the Secretary of Commerce for promulgating security standards.
6. Title 5, U.S.C., secs. 6501-6505, imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.
7. Title 15, U.S.C., Chapter 94, secs. 6801-6827. This act requires financial institutions to explain their information-sharing practices to their consumers and to safeguard sensitive data.
8. http://www.dis.arkansas.gov/security/Pages/default.aspx; http://www.state.nj.us/nj/safety/internet/; http://www.ncsl.org/research/telecommunications-and-information-technology/cyberstalking-and-cyberharassment-laws.aspx.
9. Eric A. Fischer, Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions, Congressional Research Service (9 November 2012).
10. Joint Publication (JP) 3-12(R), *Cyberspace Operations*, 5 February 2013, II-4.
11. Title 10, U.S.C., secs. 10102, 10103, 10105-10107, 10111-10113, and 12301.
12. Title 32, U.S.C., secs. 101, 109, 325, 901, 904, and 907.
13. JP 3-12(R), *Cyberspace Operations*, III-9, II-4, and Title 6, *U.S.C.*, sec. 113.
14. Title 6, U.S.C., sec. 149.
15. Title 6, U.S.C., sec. 121.
16. JP 3-12(R), *Cyberspace Operations*, II-5.
17. Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Rule 30, at 76 (Cambridge University Press, 2013).
18. Ibid., GL-4. JP 1-02 removed approval for this term. There are a total of nine contextual uses of the word "intrusion" in JP 3-12(R), with reference to "network intrusions", "intrusion or attack", "cyberspace intrusion", "prevent[ing] intrusion", "intrusion detection", "network outages/intrusions/attacks", "intrusion or attack", "prevent intrusions into DOD networks", and "[Defensive Cyberspace Operations] may be conducted in response to attack, exploitation, intrusion, or effects of malware".
19. United Nations Charter, Article 2(4).
20. Ibid., Article 51.
21. Ibid., Article 41.

22. General Keith Alexander, *Center for Strategic and International Studies (CSIS): CSIS Cybersecurity Policy Debate Series: U.S. Cybersecurity Policy and the Role of U.S. Cybercom*, Washington, D.C., (3 July 2010), 5.
23. Gary D. Solis, "Cyber Warfare," *Military Law Review*, no. 219 (Spring 2014): 22.
24. Executive Order 13010. *Critical Infrastructure Protection*, 15 July 1996.
25. Ibid.
26. Executive Order 13636. *Improving Critical Infrastructure Cybersecurity*, 12 February 2013.
27. Solis, *Cyber Warfare*, 15.
28. Schmitt, *Tallinn Manual*, 45.
29. Solis, *Cyber Warfare*, 19.
30. Ibid., 25. This citation summarizes Solis's reference to Presidential Policy Directive (PPD) 20. PPD 20 is a classified document; however, according to Solis, portions exist in the public domain at several websites including Wikipedia. Regardless, the author neither reviewed nor incorporated directly any portions of PPD 20.
31. Executive Order 13231. *Critical Infrastructure Protection in the Information Age*, 16 October 2001.
32. Department of Defense, *Strategy for Operating in Cyberspace*, July 2011, 10.
33. Title 6, U.S.C., sec. 113.
34. Ibid., sec. 121(d)(1).
35. Ibid., secs. 121(d)(3) and 121(d)(5).
36. Ibid., sec. 121(d)(6).
37. Ibid., sec. 121.
38. Ibid.
39. Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Resilience*, 12 February 2013.
40. PPD 21 and Department of Homeland Security, *National Infrastructure Protection Plan (NIPP): Partnering for Critical Infrastructure Security and Resilience*, 2013, 11.
41. NIPP, 10.
42. Ibid., 13.
43. Ibid.
44. Ibid.
45. Ibid., 14.
46. Ibid., 15.
47. Ibid.
48. Ibid., 16.
49. Ibid., 15.
50. Ibid., 21.
51. Ibid., 22.
52. Ibid.
53. Ibid., 23.
54. Executive Order: *Promoting Private Sector Cybersecurity Information Sharing*, 13 February 2015.
55. Ibid.
56. Ibid.
57. Ibid.

58. *NIPP: IT Sector Specific Plan Annex* (2010), 13.
59. Ibid., 15.
60. *NIPP: Chemical Sector-Specific Plan* (2010), 25.
61. http://www.ngaus.org/issues-advocacy/priorities-issues/fund-guard-cyber-force.
62. *National Defense Authorization Act of 2014*. HR 3304, 113th Congress, 2014.
63. Ibid.
64. Ibid.
65. http://www.ngaus.org/issues-advocacy/priorities-issues/fund-guard-cyber-force.
66. Ibid.
67. 32 U.S.C. sec. 102.
68. *Michie's Alabama Code Annotated*, 31-2-112 (2014).
69. *Alaska Statutes*, 26.05.070 (2014).
70. *Arkansas Code*, 12-61-111 (2014); *Deering's California Code Annotated*, California Military and Veteran's Code, sec 146 (2015); *Connecticut General Statutes*, sec 27-16 (2014); *Delaware Code Annotated*, 20 Delaware Code, sec 171 (2015); *Missouri Annotated Statutes*, 41.490 (2014); *Rhode Island General Laws*, sec 30-206 (2014); and *Revised Code of Washington* sec. 38.08.040 (2014).
71. *Arizona Revised Statutes*, 26-301 and 26-303 (2014).
72. *Michigan Compiled Laws Service* (MCLS), sec 32.551 (2014).
73. MCLS, sec. 32.505.
74. *Virginia Code Annotated*, sec. 44-75.1 (2014).
75. http://www.nationalguard.mil/News/ArticleView/tabid/5563/Article/3701/missouri-national-guard-forming-full-time-cyber-security-unit.aspx.
76. http://www.delawarenationalguard.com/members/air/166nws/.
77. National Governors Association, *Act and Adjust: A Call to Action for Governors for Cybersecurity*, September 2013, 4.
78. Ibid.
79. Ibid.
80. http://www.homelandsecuritynewswire.com/dr20111219-national-guardsmen-the-new-front-line-in-cybersecurity.
81. http://news.minationalguard.com/2015/02/25/michigan-selected-for-army-national-guard-cyber-protection-team/.
82. Ibid.
83. Rick Snyder, *Michigan Cyber Initiative 2015 – Leading the Nation: An Interagency, Public-Private Collaboration* (2015), 4.
84. Ibid.
85. Ibid., 7.
86. Ibid., 9.
87. Ibid.
88. Ibid.
89. Ibid., 11.
90. Ibid., 16.
91. Ibid.
92. Ibid., 17.
93. Ibid., 18.

94. Ibid.
95. Ibid.
96. Ibid., 19.
97. Ibid.
98. Ibid.
99. Title 18, U.S.C., sec. 1385. The Posse Comitatus Act prohibits Title 10 military forces from enforcing domestic criminal laws, except as permitted by the Constitution or otherwise directed by Congress.

Bibliography

Alaska Statutes. Section 26.05.070, 2014.

Alexander, Keith. *Center for Strategic and International Studies (CSIS): CSIS Cybersecurity Policy Debate Series: U.S. Cybersecurity Policy and the Role of U.S. CYBERCOM*, Washington, D.C., 3 July 2010.

Arizona Revised Statutes. Sections 26-301 and 26-303, 2014.

Arkansas Code. Section 12-16-111, 2014.

Arkansas Department of Information Systems. http://www.dis.arkansas.gov/security/Pages/default.aspx.

Charter of the United Nations and Statute of the International Court of Justice. San Francisco, CA, 1945.

Cieply, Michael and Brooks Barnes. "Sony Pictures Demands That News Agencies Delete 'Stolen' Data." *New York Times*, 14 December 2014.

Deering's California Code Annotated. California Military and Veteran's Code, sec. 146, 2015.

Delaware Code. 20 Delaware Code, sec. 171, 2015.

Delaware National Guard. http://www.delawarenationalguard.com/members/air/166nws/.

Department of Defense. *Strategy for Operating in Cyberspace*, July 2011.

Department of Homeland Security. *Banking and Finance Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010.

Department of Homeland Security. *Chemical Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010.

Department of Homeland Security. *Commercial Facilities Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010.

Department of Homeland Security. *Communications Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010.

Department of Homeland Security. *Critical Manufacturing Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010.

Department of Homeland Security. *Dams Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010.

Department of Homeland Security. *Defense Industrial Base Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010.

Department of Homeland Security. *Education Facilities Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010.

Department of Homeland Security. *Emergency Services Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010.

Department of Homeland Security. *Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010.

Department of Homeland Security. *Food Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010.

Department of Homeland Security. *Healthcare and Public Health Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010.

Department of Homeland Security. *Information Technology Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010.

Department of Homeland Security. *National Infrastructure Protection Plan (NIPP): Partnering for Critical Infrastructure Security and Resilience*, 2013.

Department of Homeland Security. *Nuclear Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010.

Department of Homeland Security. *Transportation System Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010.

Department of Homeland Security. *Water Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010.

Executive Order 13010. *Critical Infrastructure Protection*, 15 July 1996.

Executive Order 13231. *Critical Infrastructure Protection in the Information Age*, 16 October 2001.

Executive Order 13636. *Improving Critical Infrastructure Cybersecurity*, 12 February 2013.

Executive Order – *Promoting Private Sector Cybersecurity Information Sharing*, 13 February 2015.

Fischer, Eric A. "Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions," *Congressional Research Service* (9 November 2012).

Homeland Security Newswire. http://www.homelandsecuritynewswire.com/dr20111219-national-guardsmen-the-new-front-line-in-cybersecurity.

Joint Publication 3-12(R). *Cyberspace Operations*, 5 February 2013.

Michie's Alabama Code Annotated. Section 31-2-112, 2014.

Michigan Compiled Laws Service. Section 32.551, 2014.

Michigan National Guard News. http://news.minationalguard.com/2015/02/25/michigan-selected-for-army-national-guard-cyber-protection-team/.

Missouri Annotated Statutes. Section 41.490, 2014.

National Conference of State Legislatures. http://www.ncsl.org/research/telecommunications-and-information-technology/cyberstalking-and-cyberharassment-laws.aspx.

National Governors Association. *Act and Adjust: A Call to Action for Governors for Cybersecurity*, September 2013.

National Guard. http://www.nationalguard.mil/News/ArticleView/tabid/5563/Article/574213/missouri-national-guard-forming-full-time-cyber-security-unit.aspx.

National Guard Association of the United States. http://www.ngaus.org/issues-advocacy/priorities-issues/fund-guard-cyber-force.

Official Website for the State of New Jersey. http://www.state.nj.us/nj/safety/internet/.

Presidential Policy Directive (PPD) 21. *Critical Infrastructure Security and Resilience*, 12 February 2013.

Revised Code of Washington. Section 38.08.040, 2014.

Rhode Island General Laws. Section 30-206, 2014.

Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge, UK: Cambridge University Press, 2013.

Solis, Gary D. "Cyber Warfare." *Military Law Review*, no. 219 (Spring 2014).

"Sony Pictures Entertainment Notice Letter." 8 December 2014

Snyder, Rick. *Michigan Cyber Initiative 2015 – Leading the Nation: An Interagency, Public-Private Collaboration*, 2015.

Title 5, United States Code (U.S.C.), secs. 6501-6505.

Title 6, U.S.C., secs. 113, 121, and 149.

Title 10, U.S.C., secs. 10102, 10103, 10105-1017, 10111-10113, 12301,

Title 15, U.S.C., secs. 272, 6801-6827, and 7704.

Title 18, U.S.C., sec. 1385.

Title 32, U.S.C., secs. 101, 102, 109, 325, 901, 904, and 907.

US House. *National Defense Authorization Act, 2014*. 113th Congress, 2014. H. R. 3304.

Virginia Code Annotated. Section 44-75.1, 2014.